EXHIBIT “C”

From: threat-notifications@apple.com
Date: November 23, 2021 at 5:05:30 PM AST
To: franco6020@icloud.com
Subject: ALERT: State-sponsored attackers may be targeting your iPhone

ALERT: State-sponsored attackers may be targeting your iPhone

Apple believes you are being targeted by state-sponsored attackers who are trying to remotely compromise the iPhone associated with your Apple ID franco6020@icloud.com. These attackers are likely targeting you individually because of who you are or what you do. If your device is compromised by a state-sponsored attacker, they may be able to remotely access your sensitive data, communications, or even the camera and microphone. While it's possible this is a false alarm, please take this warning seriously.

Apple recommends that you immediately take these actions:

- **Update your iPhone to the latest software version, iOS 15.1.1.** We believe the state-sponsored attacks we detected are ineffective against iOS 15 and later, and urge you to always update to the latest software as soon as it's available.
- **Enlist expert help** such as the rapid-response emergency security assistance provided by the Digital Security Helpline at the nonprofit Access Now. You can contact them 24 hours a day, seven days a week through their website*: accessnow . org / help.

State-sponsored attackers are very well-funded and sophisticated, and their attacks evolve over time. Researchers and journalists have publicly documented such attacks against popular cloud services, including iMessage as well as Facebook Messenger, Gmail, Signal, and WhatsApp. Some state-sponsored attacks need no interaction from you, and others rely on tricking you into clicking a malicious link or opening an attachment in an email, SMS, or other

message. These attempts can be quite convincing, ranging from fake package tracking updates to custom-crafted, emotional appeals claiming a named family member is in danger. **Be cautious with all links you receive, and don't open any links or attachments from unexpected or unknown senders.**

State-sponsored attackers are sophisticated and will likely try to attack you through other channels, devices, and accounts not associated with Apple. Experts can provide the best advice for your specific circumstance, but if you are unable to reach an expert, consider the following additional precautions:

- **Sign out of all messaging and cloud services**, including those that were used in previous state-sponsored attacks, some of which are listed above.
- **Restore your device to factory settings.** For instructions, please look up Apple support article HT201252 on support . apple . com.
- **Change your passwords for any sensitive websites and services** that you have accessed from your iPhone.

We are unable to provide more information about what caused us to send you this notification, as that may help state-sponsored attackers adapt their behavior to evade detection in the future. Apple threat notifications like this one will never ask you to click any links, install an app or profile, or provide your Apple ID password or verification code by email or over the phone.

To verify that an Apple threat notification is genuine, sign in to appleid.apple.com. If Apple sent you a threat notification, it will be clearly visible at the top of the page after you sign in. Please do not reply to this notification. We are unable to monitor responses to this message.

*Spaces inserted into all URLs to avoid creation of links. Please retype without spaces into a browser.